Defense Information Systems Agency
Joint Information & Engineering Organization
Center for Information Technology Standards

http://www-pki.itsi.disa.mil/

23 June 2000

State Analysis of Certification Path Processing Procedures

Purpose:

Analyze the states entered by the path validation procedures defined in current and developing standards.

Conditions:

For purposes of analysis, Pa, Pb, and Pc define policy OIDs.

Certificates are constructed per DoD Class 3 PKI Interface Specification, v1.01, dated 8 May 2000.

It is assumed that clients will process non-critical extensions rather than ignore them. If not, the client will not perform the defined path processing procedures.

Summary of Certification Path Processing Analyses:

X.509v3 Procedure

Case	Root CA cites polices	Signing CA cites polices	*initial-explicit-policy* set	*initial-policy-set*	Result
1	F	T	T	Pa	Failed
2	F	T	F	Pa	Succeeded
3	F	T	F	Pb	Failed
4	F	F	F	Pa	Succeeded
5	F	F	F	Pb	Failed
6	T	T	T	Pa	Succeeded
7	T	T	F	Pa	Succeeded
8	T	F	T	Pa	Failed

RFC 2459 Procedure

Case	Root CA cites polices	Signing CA cites polices	*initial-policy-set*	Result
1	F	T	Pa	Conditional Success
2	T	T	Pa	Succeeded
3	T	T	Pb	Failed
4	T	F	Pa	Conditional Success
5	T	F	Pb	Failed

DoD PKI Procedure

Case	Root CA cites polices	Signing CA cites polices	*initial-policy-set*	Result
1	F	T	Pa	Conditional Success
2	T	T	Pa	Succeeded
3	T	T	Pb	Failed
4	T	F	Pa	Conditional Success
5	T	F	Pb	Failed

X.509v4 Procedure

Case	Root CA cites polices	Signing CA cites polices	*initial-explicit-policy* set	*initial-policy-set*	Result
1	F	T	T	Pa	Failed
2	F	T	F	Pa	Failed
3	T	T	T	Pa	Succeeded
4	T	T	F	Pa	Succeeded
5	T	F	T	Pa	Failed
6	T	F	F	Pa	Failed
7	T	T	T	Pb	Conditional Success
8	T	T	F	Pb	Conditional Success

Revised RFC 2459 Procedure

Case	Root CA cites polices	Signing CA cites polices	initial-explicit-policy set	user_initial_policy_set	Result
1	F	T	T	Pa	Failed
2	F	T	F	Pa	Failed
3	T	T	T	Pa	Succeeded
4	T	T	F	Pa	Succeeded
5	T	F	T	Pa	Failed
6	T	F	F	Pa	Failed
7	T	T	T	Pb	Failed
8	T	T	F	Pb	Failed

Conclusions:

X.509v3, RFC 2459 and DoD PKI path processing procedures are dependent on the certificate policies extension being populated and critical. Not using the extension or not setting it to critical in all certificates in the path creates conditions that are open to implementers' interpretation. An implementer may decide that:

a) In the absence of certificate policies extension, terminate the procedure and return a failure indication.

b) In the absence of certificate policies, set either *authority-constrained policy-set* or acceptable policy set to NULL and continue processing the path. The procedure will then fail at a later check.

c) In the absence of certificate policies, leave either *authority-constrained policy-set* or acceptable policy in their current states. The path processing will then continue to successful completion.

d) On encountering non-critical certificate policies, terminate the procedure and return failure.

e) On encountering non-critical certificate policies, handle it in the same manner as if it were critical.

For X.509v4 path processing to be successful, the certificate policies extension must be present in all certificates in the path. The X.509v4 procedure returns a success indication even if the end certificate does not have an acceptable policy OID. The RP will have to compare its *initial-policy-set* against the

returned NULL set in the *user-constrained-policy-set* in order to understand that the end certificate does not have an acceptable policy OID.

For the revised RFC 2459 path processing procedure to be successful, the certificate policies extension must be present in all certificates in the path.

Gregor Scott
JIEO-JEBBB
Ft. Monmouth, NJ 07703-5613
732-427-6856
scottg@ftm.disa.mil

X.509v3 procedure

Reference: X.509v3, The Directory: Authentication Framework, 06/97, section 12.4.3.

Case 1: Signing CA cites policies. RP sets *initial-explicit-policy*.

RP Inputs:
- Certification Path: Root - CA-1 - Signer
- Trusted public key: Root public key
- *initial-policy-set*: Pa
- *initial-explicit-policy*: T
- *initial-policy-mapping-inhibit*: T
- Current date/time

Initialize State Variables:
- *user-constrained-policy-set*: Pa
- *authority-constrained-policy-set*: *any-policy*
- *permitted-subtrees*: *unbounded*
- *excluded-subtrees*: empty
- *explicit-policy-indicator*: T
- *policy-mapping-inhibit-indicator*: T
- *explicit-policy-pending*: unset
- *policy-mapping-inhibit-pending*: unset

DoD Root CA Certificate
- Issuer: Class 3 Root CA
- Subject: Class 3 Root CA
- certificatePolicies: not used
- policyMappings: not used
- basicconstraints: cA = T pLC = Not used c = F
- nameConstraints: not used
- policyConstraints: not used

Status: Failed

Reason: The *explicit-policy-indicator* was set, *user-constrained-policy-set* was set to Pa, and Root certificate certificatePolicies did not contain Pa. (check c)

Case 2: Signing CA cites policies. RP does not set *initial-explicit-policy*.

RP Inputs:
- Certification Path: Root - CA-1 - Signer
- Trusted public key: Root public key
- *initial-policy-set*: Pa
- *initial-explicit-policy*: F
- *initial-policy-mapping-inhibit*: T
- Current date/time

⬇

Initialize State Variables:
- *user-constrained-policy-set*: Pa
- *authority-constrained-policy-set*: *any-policy*
- *permitted-subtrees*: *unbounded*
- *excluded-subtrees*: empty
- *explicit-policy-indicator*: F
- *policy-mapping-inhibit-indicator*: T
- *explicit-policy-pending*: unset
- *policy-mapping-inhibit-pending*: unset

⬇

DoD Root CA Certificate
- Issuer: Class 3 Root CA
- Subject: Class 3 Root CA
- certificatePolicies: not used
- policyMappings: not used
- basicconstraints: cA = T pLC = Not used c = F
- nameConstraints: not used
- policyConstraints: not used

⬇

State Variables:
- *user-constrained-policy-set*: Pa
- *authority-constrained-policy-set*: *any-policy*
- *permitted-subtrees*: *unbounded*
- *excluded-subtrees*: empty
- *explicit-policy-indicator*: F
- *policy-mapping-inhibit-indicator*: T
- *explicit-policy-pending*: unset
- *policy-mapping-inhibit-pending*: unset

⬇

```
Signing CA Certificate 1
    Issuer: Class 3 Root CA
    Subject: Class 3 CA-1
    certificatePolicies: Pa, Pb, Pc  qualifiers: no  c = F
    policyMappings: not used
    basicConstraints:    cA = T    pLC = not used     c = T
    nameConstraints: not used
    policyConstraints:                                c = F
        requiredExplicitPolicy       SkipCerts = 0
        inhibitPolicyMapping         SkipCerts = 0
```

```
State Variables:
   user-constrained-policy-set: Pa
   authority-constrained-policy-set: Pa, Pb, Pc
   permitted-subtrees: unbounded
   excluded-subtrees: empty
   explicit-policy-indicator: T
   policy-mapping-inhibit-indicator: T
   explicit-policy-pending: unset
   policy-mapping-inhibit-pending: unset
```

```
Signature Certificate
    Issuer: Class 3 CA-1
    Subject: Signer
    certificatePolicies: Pa          qualifiers: no  c = F
    policyMappings: not used
    nameConstraints: not used
    policyConstraints: not used
```

```
State Variables:
   user-constrained-policy-set: Pa
   authority-constrained-policy-set: Pa
   permitted-subtrees: unbounded
   excluded-subtrees: empty
   explicit-policy-indicator: T
   policy-mapping-inhibit-indicator: T
   explicit-policy-pending: unset
   policy-mapping-inhibit-pending: unset
```

Status: Succeeded. The intersection of *authority-constrained-policy-set* and *user-constrained-policy-set* is not empty.

Case 3: Signing CA cites policies. RP does not set *initial-explicit-policy*. RP sets *initial-policy-set* to Pb.

RP Inputs:
- Certification Path: Root - CA-1 - Signer
- Trusted public key: Root public key
- *initial-policy-set*: Pb
- *initial-explicit-policy*: F
- *initial-policy-mapping-inhibit*: T
- Current date/time

Initialize State Variables:
- *user-constrained-policy-set*: Pb
- *authority-constrained-policy-set*: *any-policy*
- *permitted-subtrees*: *unbounded*
- *excluded-subtrees*: empty
- *explicit-policy-indicator*: F
- *policy-mapping-inhibit-indicator*: T
- *explicit-policy-pending*: unset
- *policy-mapping-inhibit-pending*: unset

DoD Root CA Certificate
- Issuer: Class 3 Root CA
- Subject: Class 3 Root CA
- certificatePolicies: not used
- policyMappings: not used
- basicconstraints: cA = T pLC = Not used c = F
- nameConstraints: not used
- policyConstraints: not used

State Variables:
- *user-constrained-policy-set*: Pb
- *authority-constrained-policy-set*: *any-policy*
- *permitted-subtrees*: *unbounded*
- *excluded-subtrees*: empty
- *explicit-policy-indicator*: F
- *policy-mapping-inhibit-indicator*: T
- *explicit-policy-pending*: unset
- *policy-mapping-inhibit-pending*: unset

```
Signing CA Certificate 1
    Issuer: Class 3 Root CA
    Subject: Class 3 CA-1
    certificatePolicies: Pa, Pb, Pc  qualifiers: no  c = F
    policyMappings: not used
    basicConstraints:    cA = T    pLC = not used     c = T
    nameConstraints: not used
    policyConstraints:                                c = F
        requiredExplicitPolicy       SkipCerts = 0
        inhibitPolicyMapping         SkipCerts = 0
```

```
State Variables:
   user-constrained-policy-set: Pb
   authority-constrained-policy-set: Pa, Pb, Pc
   permitted-subtrees: unbounded
   excluded-subtrees: empty
   explicit-policy-indicator: T
   policy-mapping-inhibit-indicator: T
   explicit-policy-pending: unset
   policy-mapping-inhibit-pending: unset
```

```
Signature Certificate
    Issuer: Class 3 CA-1
    Subject: Signer
    certificatePolicies: Pa          qualifiers: no  c = F
    policyMappings: not used
    nameConstraints: not used
    policyConstraints: not used
```

Status: Failed.

Reason: Certificate policies extension does not contain the policy OID (Pb) cited in *user-constrained-policy-set* (check c).

Case 4: Signing CA does not cite policies. RP does not set *initial-explicit-policy*.

RP Inputs:
- Certification Path: Root - CA-2 - Signer
- Trusted public key: Root public key
- *initial-policy-set*: Pa
- *initial-explicit-policy*: F
- *initial-policy-mapping-inhibit*: T
- Current date/time

Initialize State Variables:
- *user-constrained-policy-set*: Pa
- *authority-constrained-policy-set*: *any-policy*
- *permitted-subtrees*: *unbounded*
- *excluded-subtrees*: empty
- *explicit-policy-indicator*: F
- *policy-mapping-inhibit-indicator*: T
- *explicit-policy-pending*: unset
- *policy-mapping-inhibit-pending*: unset

DoD Root CA Certificate
- Issuer: Class 3 Root CA
- Subject: Class 3 Root CA
- certificatePolicies: not used
- policyMappings: not used
- basicconstraints: cA = T pLC = Not used c = F
- nameConstraints: not used
- policyConstraints: not used

State Variables:
- *user-constrained-policy-set*: Pa
- *authority-constrained-policy-set*: *any-policy*
- *permitted-subtrees*: *unbounded*
- *excluded-subtrees*: empty
- *explicit-policy-indicator*: F
- *policy-mapping-inhibit-indicator*: T
- *explicit-policy-pending*: unset
- *policy-mapping-inhibit-pending*: unset

```
Signing CA Certificate 2
    Issuer: Class 3 Root CA
    Subject: Class 3 CA-2
    certificatePolicies: none cited
    policyMappings: not used
    basicConstraints:    cA = T    pLC = not used     c = T
    nameConstraints: not used
    policyConstraints:                                c = F
        requiredExplicitPolicy       SkipCerts = 0
        inhibitPolicyMapping         SkipCerts = 0
```

```
State Variables:
   user-constrained-policy-set: Pa
   authority-constrained-policy-set: any-policy
   permitted-subtrees: unbounded
   excluded-subtrees: empty
   explicit-policy-indicator: T
   policy-mapping-inhibit-indicator: T
   explicit-policy-pending: unset
   policy-mapping-inhibit-pending: unset
```

```
Signature Certificate
    Issuer: Class 3 CA-1
    Subject: Signer
    certificatePolicies: Pa          qualifiers: no  c = F
    policyMappings: not used
    nameConstraints: not used
    policyConstraints: not used
```

```
State Variables:
   user-constrained-policy-set: Pa
   authority-constrained-policy-set: Pa
   permitted-subtrees: unbounded
   excluded-subtrees: empty
   explicit-policy-indicator: T
   policy-mapping-inhibit-indicator: T
   explicit-policy-pending: unset
   policy-mapping-inhibit-pending: unset
```

Status: Succeeded. The intersection of *authority-constrained-policy-set* and *user-constrained-policy-set* is not empty.

Case 5: Signing CA does not cite policies. RP does not set *initial-explicit-policy*. RP sets *initial-policy-set* to Pb.

RP Inputs:
- Certification Path: Root - CA-2 - Signer
- Trusted public key: Root public key
- *initial-policy-set*: Pb
- *initial-explicit-policy*: F
- *initial-policy-mapping-inhibit*: T
- Current date/time

Initialize State Variables:
- *user-constrained-policy-set*: Pb
- *authority-constrained-policy-set*: *any-policy*
- *permitted-subtrees*: *unbounded*
- *excluded-subtrees*: empty
- *explicit-policy-indicator*: F
- *policy-mapping-inhibit-indicator*: T
- *explicit-policy-pending*: unset
- *policy-mapping-inhibit-pending*: unset

DoD Root CA Certificate
- Issuer: Class 3 Root CA
- Subject: Class 3 Root CA
- certificatePolicies: not used
- policyMappings: not used
- basicconstraints: cA = T pLC = Not used c = F
- nameConstraints: not used
- policyConstraints: not used

State Variables:
- *user-constrained-policy-set*: Pb
- *authority-constrained-policy-set*: *any-policy*
- *permitted-subtrees*: *unbounded*
- *excluded-subtrees*: empty
- *explicit-policy-indicator*: F
- *policy-mapping-inhibit-indicator*: T
- *explicit-policy-pending*: unset
- *policy-mapping-inhibit-pending*: unset

```
Signing CA Certificate 2
    Issuer: Class 3 Root CA
    Subject: Class 3 CA-2
    certificatePolicies: not used
    policyMappings: not used
    basicConstraints:    cA = T    pLC = not used     c = T
    nameConstraints: not used
    policyConstraints:                                c = F
        requiredExplicitPolicy       SkipCerts = 0
        inhibitPolicyMapping         SkipCerts = 0
```

```
State Variables:
   user-constrained-policy-set: Pb
   authority-constrained-policy-set: any-policy
   permitted-subtrees: unbounded
   excluded-subtrees: empty
   explicit-policy-indicator: T
   policy-mapping-inhibit-indicator: T
   explicit-policy-pending: unset
   policy-mapping-inhibit-pending: unset
```

```
Signature Certificate
    Issuer: Class 3 CA-1
    Subject: Signer
    certificatePolicies: Pa          qualifiers: no  c = F
    policyMappings: not used
    nameConstraints: not used
    policyConstraints: not used
```

Status: Failed.

Reason: Certificate policies extension does not contain the policy OID (Pb) cited in *user-constrained-policy-set* (check c).

Case 6: Root CA cites policies. Signing CA cites policies. RP does set *initial-explicit-policy*.

RP Inputs:
- Certification Path: Root - CA-1 - Signer
- Trusted public key: Root public key
- *initial-policy-set*: Pa
- *initial-explicit-policy*: T
- *initial-policy-mapping-inhibit*: T
- Current date/time

Initialize State Variables:
- *user-constrained-policy-set*: Pa
- *authority-constrained-policy-set*: *any-policy*
- *permitted-subtrees*: *unbounded*
- *excluded-subtrees*: empty
- *explicit-policy-indicator*: T
- *policy-mapping-inhibit-indicator*: T
- *explicit-policy-pending*: unset
- *policy-mapping-inhibit-pending*: unset

DoD Root CA Certificate
- Issuer: Class 3 Root CA
- Subject: Class 3 Root CA
- certificatePolicies: Pa, Pb, Pc qualifiers: no c = F
- policyMappings: not used
- basicconstraints: cA = T pLC = Not used c = F
- nameConstraints: not used
- policyConstraints: not used

State Variables:
- *user-constrained-policy-set*: Pa
- *authority-constrained-policy-set*: Pa, Pb, Pc
- *permitted-subtrees*: *unbounded*
- *excluded-subtrees*: empty
- *explicit-policy-indicator*: T
- *policy-mapping-inhibit-indicator*: T
- *explicit-policy-pending*: unset
- *policy-mapping-inhibit-pending*: unset

```
Signing CA Certificate 1
    Issuer: Class 3 Root CA
    Subject: Class 3 CA-1
    certificatePolicies: Pa, Pb, Pc  qualifiers: no  c = F
    policyMappings: not used
    basicConstraints:    cA = T    pLC = not used     c = T
    nameConstraints: not used
    policyConstraints:                                c = F
        requiredExplicitPolicy       SkipCerts = 0
        inhibitPolicyMapping         SkipCerts = 0
```

```
State Variables:
   user-constrained-policy-set: Pa
   authority-constrained-policy-set: Pa, Pb, Pc
   permitted-subtrees: unbounded
   excluded-subtrees: empty
   explicit-policy-indicator: T
   policy-mapping-inhibit-indicator: T
   explicit-policy-pending: unset
   policy-mapping-inhibit-pending: unset
```

```
Signature Certificate
    Issuer: Class 3 CA-1
    Subject: Signer
    certificatePolicies: Pa          qualifiers: no  c = F
    policyMappings: not used
    nameConstraints: not used
    policyConstraints: not used
```

```
State Variables:
   user-constrained-policy-set: Pa
   authority-constrained-policy-set: Pa
   permitted-subtrees: unbounded
   excluded-subtrees: empty
   explicit-policy-indicator: T
   policy-mapping-inhibit-indicator: T
   explicit-policy-pending: unset
   policy-mapping-inhibit-pending: unset
```

Status: Succeeded. The intersection of *authority-constrained-policy-set* and *user-constrained-policy-set* is not empty.

Case 7: Root CA cites policies. Signing CA cites policies. RP does not set *initial-explicit-policy*.

RP Inputs:
- Certification Path: Root - CA-1 - Signer
- Trusted public key: Root public key
- *initial-policy-set*: Pa
- *initial-explicit-policy*: F
- *initial-policy-mapping-inhibit*: T
- Current date/time

Initialize State Variables:
- *user-constrained-policy-set*: Pa
- *authority-constrained-policy-set*: *any-policy*
- *permitted-subtrees*: *unbounded*
- *excluded-subtrees*: empty
- *explicit-policy-indicator*: F
- *policy-mapping-inhibit-indicator*: T
- *explicit-policy-pending*: unset
- *policy-mapping-inhibit-pending*: unset

DoD Root CA Certificate
- Issuer: Class 3 Root CA
- Subject: Class 3 Root CA
- certificatePolicies: Pa, Pb, Pc qualifiers: no c = F
- policyMappings: not used
- basicconstraints: cA = T pLC = Not used c = F
- nameConstraints: not used
- policyConstraints: not used

State Variables:
- *user-constrained-policy-set*: Pa
- *authority-constrained-policy-set*: Pa, Pb, Pc
- *permitted-subtrees*: *unbounded*
- *excluded-subtrees*: empty
- *explicit-policy-indicator*: F
- *policy-mapping-inhibit-indicator*: T
- *explicit-policy-pending*: unset
- *policy-mapping-inhibit-pending*: unset

```
Signing CA Certificate 1
    Issuer: Class 3 Root CA
    Subject: Class 3 CA-1
    certificatePolicies: Pa, Pb, Pc  qualifiers: no  c = F
    policyMappings: not used
    basicConstraints:    cA = T    pLC = not used     c = T
    nameConstraints: not used
    policyConstraints:                                c = F
        requiredExplicitPolicy       SkipCerts = 0
        inhibitPolicyMapping         SkipCerts = 0
```

```
State Variables:
   user-constrained-policy-set: Pa
   authority-constrained-policy-set: Pa, Pb, Pc
   permitted-subtrees: unbounded
   excluded-subtrees: empty
   explicit-policy-indicator: T
   policy-mapping-inhibit-indicator: T
   explicit-policy-pending: unset
   policy-mapping-inhibit-pending: unset
```

```
Signature Certificate
    Issuer: Class 3 CA-1
    Subject: Signer
    certificatePolicies: Pa          qualifiers: no  c = F
    policyMappings: not used
    nameConstraints: not used
    policyConstraints: not used
```

```
State Variables:
   user-constrained-policy-set: Pa
   authority-constrained-policy-set: Pa
   permitted-subtrees: unbounded
   excluded-subtrees: empty
   explicit-policy-indicator: T
   policy-mapping-inhibit-indicator: T
   explicit-policy-pending: unset
   policy-mapping-inhibit-pending: unset
```

Status: Succeeded. The intersection of *authority-constrained-policy-set* and *user-constrained-policy-set* is not empty.

Case 8: Root CA cites policies. Signing CA does not cite policies. RP does set *initial-explicit-policy*.

RP Inputs:
- Certification Path: Root - CA-1 - Signer
- Trusted public key: Root public key
- *initial-policy-set*: Pa
- *initial-explicit-policy*: T
- *initial-policy-mapping-inhibit*: T
- Current date/time

Initialize State Variables:
- *user-constrained-policy-set*: Pa
- *authority-constrained-policy-set*: *any-policy*
- *permitted-subtrees*: *unbounded*
- *excluded-subtrees*: empty
- *explicit-policy-indicator*: T
- *policy-mapping-inhibit-indicator*: T
- *explicit-policy-pending*: unset
- *policy-mapping-inhibit-pending*: unset

DoD Root CA Certificate
- Issuer: Class 3 Root CA
- Subject: Class 3 Root CA
- certificatePolicies: Pa, Pb, Pc qualifiers: no c = F
- policyMappings: not used
- basicconstraints: cA = T pLC = Not used c = F
- nameConstraints: not used
- policyConstraints: not used

State Variables:
- *user-constrained-policy-set*: Pa
- *authority-constrained-policy-set*: Pa, Pb, Pc
- *permitted-subtrees*: *unbounded*
- *excluded-subtrees*: empty
- *explicit-policy-indicator*: T
- *policy-mapping-inhibit-indicator*: T
- *explicit-policy-pending*: unset
- *policy-mapping-inhibit-pending*: unset

```
Signing CA Certificate 1
    Issuer: Class 3 Root CA
    Subject: Class 3 CA-1
    certificatePolicies: not used
    policyMappings: not used
    basicConstraints:    cA = T    pLC = not used     c = T
    nameConstraints: not used
    policyConstraints:                                c = F
        requiredExplicitPolicy       SkipCerts = 0
        inhibitPolicyMapping         SkipCerts = 0
```

Status: Failed.

Reason: Certificate policies extension does not contain the policy OID (Pa) cited in *user-constrained-policy-set* (check c).

RFC 2459 Procedure

Reference: RFC 2459, Internet X.509 Public Key Infrastructure Certificate and CRL Profile, January 1999, section 6.1.

Case 1: Root CA does not cite policies. Signing CA cites policies. RP cites policy Pa.

RP Inputs:
- Certification Path: Root - CA-1 - Signer
- Trusted public key: Root public key
- *initial-policy-set*: Pa
- Current date/time
- Time for which path validation should be determined.

Initialize State Variables:
- acceptable policy set: *any-policy*
- *permitted-subtrees*: *unbounded*
- *excluded-subtrees*: empty
- *explicit-policy-pending*: unset
- *policy-mapping-inhibit-pending*: unset

DoD Root CA Certificate
- Issuer: Class 3 Root CA
- Subject: Class 3 Root CA
- keyUsage: not used
- certificatePolicies: not used
- policyMappings: not used
- basicconstraints: cA = T pLC = Not used c = F
- nameConstraints: not used
- policyConstraints: not used

Comment: Path processing check (e.1) looks for the certiciatePolicies extension. Since it is absent in this certificate, what does the processing software do? Leave the acceptable policy set as is or reset it to NULL? A setting to NULL will cause check (g) to fail and invalidate the certification path. For the validation to proceed, the absence of certiciatePolicies would have to be interpreted as having no effect on the acceptable policy set state. That is leaving acceptable policy set as is.

```
State Variables:
    acceptable policy set: any-policy
    permitted-subtrees: unbounded
    excluded-subtrees: empty
    explicit-policy-pending: unset
    policy-mapping-inhibit-pending: unset
```

```
Signing CA Certificate 1
    Issuer: Class 3 Root CA
    Subject: Class 3 CA-1
    keyUsage: DS, KCS, cRLSign                          c = T
    certificatePolicies: Pa, Pb, Pc  qualifiers: no  c = F
    policyMappings: not used
    basicConstraints:    cA = T    pLC = Not used    c = T
    nameConstraints: not used
    policyConstraints:                                  c = F
        requiredExplicitPolicy       SkipCerts = 0
        inhibitPolicyMapping         SkipCerts = 0
```

```
State Variables:
    acceptable policy set: Pa, Pb, Pc
    permitted-subtrees: unbounded
    excluded-subtrees: empty
    explicit-policy-pending: 0
    policy-mapping-inhibit-pending: 0
```

```
Signature Certificate
    Issuer: Class 3 CA-1
    Subject: Signer
    keyUsage: DS, NR                                    c = T
    certificatePolicies: Pa          qualifiers: no  c = F
    policyMappings: not used
    nameConstraints: not used
    policyConstraints: not used
```

```
State Variables:
    acceptable policy set: Pa
    permitted-subtrees: unbounded
    excluded-subtrees: empty
    explicit-policy-pending: 0
    policy-mapping-inhibit-pending: 0
```

Status: Succeeded. All path processing checks succeeded given decision discussed in comment above.

Case 2: Root CA cites policies. Signing CA cites policies. RP cites policy Pa.

RP Inputs:
    Certification Path: Root - CA-1 - Signer
    Trusted public key: Root public key
    initial-policy-set: Pa
    Current date/time
    Time for which path validation should be determined.

Initialize State Variables:
    acceptable policy set: *any-policy*
    permitted-subtrees: *unbounded*
    excluded-subtrees: empty
    explicit-policy-pending: unset
    policy-mapping-inhibit-pending: unset

DoD Root CA Certificate
    Issuer: Class 3 Root CA
    Subject: Class 3 Root CA
    keyUsage: not used
    certificatePolicies: Pa, Pb, Pc qualifiers: no c = F
    policyMappings: not used
    basicConstraints: cA = T pLC = Not used c = F
    nameConstraints: not used
    policyConstraints: not used

State Variables:
    acceptable policy set: Pa, Pb, Pc
    permitted-subtrees: *unbounded*
    excluded-subtrees: empty
    explicit-policy-pending: unset
    policy-mapping-inhibit-pending: unset

```
Signing CA Certificate 1
    Issuer: Class 3 Root CA
    Subject: Class 3 CA-1
    keyUsage: DS, KCS, cRLSign                          c = T
    certificatePolicies: Pa, Pb, Pc  qualifiers: no     c = F
    policyMappings: not used
    basicConstraints:    cA = T    pLC = Not used       c = T
    nameConstraints: not used
    policyConstraints:                                  c = F
        requiredExplicitPolicy       SkipCerts = 0
        inhibitPolicyMapping         SkipCerts = 0
```

```
State Variables:
    acceptable policy set: Pa, Pb, Pc
    permitted-subtrees: unbounded
    excluded-subtrees: empty
    explicit-policy-pending: 0
    policy-mapping-inhibit-pending: 0
```

```
Signature Certificate
    Issuer: Class 3 CA-1
    Subject: Signer
    keyUsage: DS, NR                                    c = T
    certificatePolicies: Pa          qualifiers: no     c = F
    policyMappings: not used
    nameConstraints: not used
    policyConstraints: not used
```

```
State Variables:
    acceptable policy set: Pa
    permitted-subtrees: unbounded
    excluded-subtrees: empty
    explicit-policy-pending: 0
    policy-mapping-inhibit-pending: 0
```

Status: Succeeded. All path processing checks succeeded.

Case 3: Root CA cites policies. Signing CA cites policies. RP cites policy Pb.

RP Inputs:
    Certification Path: Root - CA-1 - Signer
    Trusted public key: Root public key
    initial-policy-set: Pb
    Current date/time
    Time for which path validation should be determined.

Initialize State Variables:
    acceptable policy set: *any-policy*
    permitted-subtrees: *unbounded*
    excluded-subtrees: empty
    explicit-policy-pending: unset
    policy-mapping-inhibit-pending: unset

DoD Root CA Certificate
    Issuer: Class 3 Root CA
    Subject: Class 3 Root CA
    keyUsage: not used
    certificatePolicies: Pa, Pb, Pc qualifiers: no c = F
    policyMappings: not used
    basicConstraints: cA = T pLC = Not used c = F
    nameConstraints: not used
    policyConstraints: not used

State Variables:
    acceptable policy set: Pa, Pb, Pc
    permitted-subtrees: *unbounded*
    excluded-subtrees: empty
    explicit-policy-pending: unset
    policy-mapping-inhibit-pending: unset

```
Signing CA Certificate 1
    Issuer: Class 3 Root CA
    Subject: Class 3 CA-1
    keyUsage: DS, KCS, cRLSign                          c = T
    certificatePolicies: Pa, Pb, Pc  qualifiers: no    c = F
    policyMappings: not used
    basicConstraints:    cA = T    pLC = Not used      c = T
    nameConstraints: not used
    policyConstraints:                                  c = F
        requiredExplicitPolicy       SkipCerts = 0
        inhibitPolicyMapping         SkipCerts = 0
```

```
State Variables:
    acceptable policy set: Pa, Pb, Pc
    permitted-subtrees: unbounded
    excluded-subtrees: empty
    explicit-policy-pending: 0
    policy-mapping-inhibit-pending: 0
```

```
Signature Certificate
    Issuer: Class 3 CA-1
    Subject: Signer
    certificatePolicies: Pa          qualifiers: no   c = F
    policyMappings: not used
    nameConstraints: not used
    policyConstraints: not used
```

Status: Failed.

Reason: Path processing check (d.1) failed. The policy identifier in the certificate (Pa) did not match the policy identifier in the *initial-policy-set* (Pb).

Case 4: Root CA cites policies. Signing CA does not cite policies. RP cites policy Pa.

RP Inputs:
    Certification Path: Root - CA-1 - Signer
    Trusted public key: Root public key
    initial-policy-set: Pa
    Current date/time
    Time for which path validation should be determined.

Initialize State Variables:
    acceptable policy set: *any-policy*
    permitted-subtrees: *unbounded*
    excluded-subtrees: empty
    explicit-policy-pending: unset
    policy-mapping-inhibit-pending: unset

DoD Root CA Certificate
    Issuer: Class 3 Root CA
    Subject: Class 3 Root CA
    keyUsage: not used
    certificatePolicies: Pa, Pb, Pc qualifiers: no c = F
    policyMappings: not used
    basicConstraints: cA = T pLC = Not used c = F
    nameConstraints: not used
    policyConstraints: not used

State Variables:
    acceptable policy set: Pa, Pb, Pc
    permitted-subtrees: *unbounded*
    excluded-subtrees: empty
    explicit-policy-pending: unset
    policy-mapping-inhibit-pending: unset

```
Signing CA Certificate 1
    Issuer: Class 3 Root CA
    Subject: Class 3 CA-1
    keyUsage: DS, KCS, cRLSign                          c = T
    certificatePolicies: not used
    policyMappings: not used
    basicConstraints:    cA = T    pLC = Not used       c = T
    nameConstraints: not used
    policyConstraints:                                  c = F
        requiredExplicitPolicy       SkipCerts = 0
        inhibitPolicyMapping         SkipCerts = 0
```

Comment: Path processing check (e.1) looks for the certiciatePolicies extension. Since it is absent in this certificate, what does the processing software do? Leave the acceptable policy set as is or reset it to NULL? A setting to NULL will cause check (g) to fail and invalidate the certification path. For the validation to proceed, the absence of certiciatePolicies would have to be interpreted as having no effect on the acceptable policy set state. That is leaving acceptable policy set as is.

```
State Variables:
    acceptable policy set: Pa, Pb, Pc
    permitted-subtrees: unbounded
    excluded-subtrees: empty
    explicit-policy-pending: 0
    policy-mapping-inhibit-pending: 0
```

```
Signature Certificate
    Issuer: Class 3 CA-1
    Subject: Signer
    keyUsage: DS, NR                                    c = T
    certificatePolicies: Pa          qualifiers: no     c = F
    policyMappings: not used
    nameConstraints: not used
    policyConstraints: not used
```

State Variables:
    acceptable policy set: Pa
    permitted-subtrees: *unbounded*
    excluded-subtrees: empty
    explicit-policy-pending: 0
    policy-mapping-inhibit-pending: 0

Status: Succeeded. All path processing checks succeeded given decision discussed in comment above.

Case 5: Root CA cites policies. Signing CA does not cite policies. RP cites policy Pb.

```
RP Inputs:
    Certification Path: Root - CA-1 - Signer
    Trusted public key: Root public key
    initial-policy-set: Pb
    Current date/time
    Time for which path validation should be determined.
```

```
Initialize State Variables:
    acceptable policy set: any-policy
    permitted-subtrees: unbounded
    excluded-subtrees: empty
    explicit-policy-pending: unset
    policy-mapping-inhibit-pending: unset
```

```
DoD Root CA Certificate
    Issuer: Class 3 Root CA
    Subject: Class 3 Root CA
    keyUsage: not used
    certificatePolicies: Pa, Pb, Pc  qualifiers: no  c = F
    policyMappings: not used
    basicConstraints:    cA = T    pLC = not used    c = F
    nameConstraints: not used
    policyConstraints: not used
```

```
State Variables:
    acceptable policy set: Pa, Pb, Pc
    permitted-subtrees: unbounded
    excluded-subtrees: empty
    explicit-policy-pending: unset
    policy-mapping-inhibit-pending: unset
```

```
Signing CA Certificate 1
    Issuer: Class 3 Root CA
    Subject: Class 3 CA-1
    keyUsage: DS, KCS, cRLSign                          c = T
    certificatePolicies: not used
    policyMappings: not used
    basicConstraints:    cA = T    pLC = not used       c = T
    nameConstraints: not used
    policyConstraints:                                  c = F
        requiredExplicitPolicy       SkipCerts = 0
        inhibitPolicyMapping         SkipCerts = 0
```

Comment: Path processing check (e.1) looks for the certiciatePolicies extension. Since it is absent in this certificate, what does the processing software do? Leave the acceptable policy set as is or reset it to NULL? A setting to NULL will cause check (g) to fail and invalidate the certification path. For the validation to proceed, the absence of certiciatePolicies would have to be interpreted as having no effect on the acceptable policy set state. That is leaving acceptable policy set as is.

```
State Variables:
    acceptable policy set: Pa, Pb, Pc
    permitted-subtrees: unbounded
    excluded-subtrees: empty
    explicit-policy-pending: 0
    policy-mapping-inhibit-pending: 0
```

```
Signature Certificate
    Issuer: Class 3 CA-1
    Subject: Signer
    keyUsage: DS, NR                                    c = T
    certificatePolicies: Pa          qualifiers: no     c = F
    policyMappings: not used
    nameConstraints: not used
    policyConstraints: not used
```

Status: Failed.

Reason: Path processing check (d.1) failed. The policy identifier in the certificate (Pa) did not match the policy identifier in the *initial-policy-set* (Pb).

DoD PKI Procedure

Reference: Mitretek Systems document on DoD Class 3 Certification Path Validation, May 19, 2000

Case 1: Root CA does not cite policies. Signing CA cites policies. RP cites policy Pa.

RP Inputs:
- Certification Path: Root - CA-1 - Signer n = 3
- Trusted public key: Root public key
- *initial-policy-set*: Pa
- Current date/time

Initialize State Variables:
- acceptable policy set: *any-policy*
- *explicit-policy-pending*: 4

DoD Root CA Certificate
- Issuer: Class 3 Root CA
- Subject: Class 3 Root CA
- keyUsage: not used
- certificatePolicies: not used
- policyMappings: not used
- basicConstraints: cA = T pLC = not used c = F
- nameConstraints: not used
- policyConstraints: not used

Comment: Path processing check (c.1) looks for the certiciatePolicies extension. Since it is absent in this certificate, what does the processing software do? Leave the acceptable policy set as is or reset it to NULL? A setting to NULL will cause check (d) to fail and invalidate the certification path. For the validation to proceed, the absence of certiciatePolicies would have to be interpreted as having no effect on the acceptable policy set state. That is, leaving acceptable policy set as is.

State Variables:
- acceptable policy set: *any-policy*
- *explicit-policy-pending*: 4

```
Signing CA Certificate 1
    Issuer: Class 3 Root CA
    Subject: Class 3 CA-1
    keyUsage: DS, KCS, cRLSign                          c = T
    certificatePolicies: Pa, Pb, Pc  qualifiers: no     c = F
    policyMappings: not used
    basicConstraints:    cA = T    pLC = not used       c = T
    nameConstraints: not used
    policyConstraints:                                  c = F
        requiredExplicitPolicy       SkipCerts = 0
        inhibitPolicyMapping         SkipCerts = 0
```

```
State Variables:
    acceptable policy set: Pa, Pb, Pc
    explicit-policy-pending: 2
```

```
Signature Certificate
    Issuer: Class 3 CA-1
    Subject: Signer
    keyUsage: DS, NR                                    c = T
    certificatePolicies: Pa          qualifiers: no     c = F
    policyMappings: not used
    nameConstraints: not used
    policyConstraints: not used
```

```
State Variables:
    acceptable policy set: Pa
    explicit-policy-pending: 2
```

Status: Succeeded. All path processing checks succeeded, given the decision discussed in comment above.

Case 2: Root CA cites policies. Signing CA cites policies. RP cites policy Pa.

```
RP Inputs:
    Certification Path: Root - CA-1 - Signer          n = 3
    Trusted public key: Root public key
    initial-policy-set: Pa
    Current date/time
```

```
Initialize State Variables:
    acceptable policy set: any-policy
    explicit-policy-pending: 4
```

```
DoD Root CA Certificate
    Issuer: Class 3 Root CA
    Subject: Class 3 Root CA
    keyUsage: not used
    certificatePolicies: Pa, Pb, Pc  qualifiers: no  c = F
    policyMappings: not used
    basicConstraints:    cA = T    pLC = not used    c = F
    nameConstraints: not used
    policyConstraints: not used
```

```
State Variables:
    acceptable policy set: Pa, Pb, Pc
    explicit-policy-pending: 4
```

```
Signing CA Certificate 1
    Issuer: Class 3 Root CA
    Subject: Class 3 CA-1
    keyUsage: DS, KCS, cRLSign                        c = T
    certificatePolicies: Pa, Pb, Pc  qualifiers: no  c = F
    policyMappings: not used
    basicConstraints:    cA = T    pLC = not used    c = T
    nameConstraints: not used
    policyConstraints:                                c = F
        requiredExplicitPolicy       SkipCerts = 0
        inhibitPolicyMapping         SkipCerts = 0
```

```
State Variables:
    acceptable policy set: Pa, Pb, Pc
    explicit-policy-pending: 2
```

```
Signature Certificate
    Issuer: Class 3 CA-1
    Subject: Signer
    keyUsage: DS, NR                                    c = T
    certificatePolicies: Pa          qualifiers: no     c = F
    policyMappings: not used
    nameConstraints: not used
    policyConstraints: not used
```

```
State Variables:
    acceptable policy set: Pa
    explicit-policy-pending: 2
```

Status: Succeeded. All path processing checks succeeded.

Case 3: Root CA cites policies. Signing CA cites policies. RP cites policy Pb.

```
RP Inputs:
    Certification Path: Root - CA-1 - Signer          n = 3
    Trusted public key: Root public key
    initial-policy-set: Pb
    Current date/time
```

```
Initialize State Variables:
    acceptable policy set: any-policy
    explicit-policy-pending: 4
```

```
DoD Root CA Certificate
    Issuer: Class 3 Root CA
    Subject: Class 3 Root CA
    keyUsage: not used
    certificatePolicies: Pa, Pb, Pc  qualifiers: no  c = F
    policyMappings: not used
    basicConstraints:    cA = T    pLC = not used    c = F
    nameConstraints: not used
    policyConstraints: not used
```

```
State Variables:
    acceptable policy set: Pa, Pb, Pc
    explicit-policy-pending: 4
```

```
Signing CA Certificate 1
    Issuer: Class 3 Root CA
    Subject: Class 3 CA-1
    keyUsage: DS, KCS, cRLSign                        c = T
    certificatePolicies: Pa, Pb, Pc  qualifiers: no  c = F
    policyMappings: not used
    basicConstraints:    cA = T    pLC = not used    c = T
    nameConstraints: not used
    policyConstraints:                                c = F
        requiredExplicitPolicy       SkipCerts = 0
        inhibitPolicyMapping         SkipCerts = 0
```

```
State Variables:
    acceptable policy set: Pa, Pb, Pc
    explicit-policy-pending: 2
```

Signature Certificate		
Issuer: Class 3 CA-1		
Subject: Signer		
keyUsage: DS, NR		c = T
certificatePolicies: Pa	qualifiers: no	c = F
policyMappings: not used		
nameConstraints: not used		
policyConstraints: not used		

Status: Failed.

Reason: Path processing check (b.1) failed. The policy identifier in the certificate, Pa, did not match the initial policy set, Pb.

Case 4: Root CA cites policies. Signing CA does not cite policies. RP cites policy Pa.

```
RP Inputs:
    Certification Path: Root - CA-1 - Signer          n = 3
    Trusted public key: Root public key
    initial-policy-set: Pa
    Current date/time
```

```
Initialize State Variables:
    acceptable policy set: any-policy
    explicit-policy-pending: 4
```

```
DoD Root CA Certificate
    Issuer: Class 3 Root CA
    Subject: Class 3 Root CA
    keyUsage: not used
    certificatePolicies: Pa, Pb, Pc  qualifiers: no  c = F
    policyMappings: not used
    basicConstraints:    cA = T    pLC = not used    c = F
    nameConstraints: not used
    policyConstraints: not used
```

```
State Variables:
    acceptable policy set: Pa, Pb, Pc
    explicit-policy-pending: 4
```

```
Signing CA Certificate 1
    Issuer: Class 3 Root CA
    Subject: Class 3 CA-1
    keyUsage: DS, KCS, cRLSign                        c = T
    certificatePolicies: not used
    policyMappings: not used
    basicConstraints:    cA = T    pLC = not used    c = T
    nameConstraints: not used
    policyConstraints:                                c = F
        requiredExplicitPolicy       SkipCerts = 0
        inhibitPolicyMapping         SkipCerts = 0
```

Comment: Path processing check (c.1) looks for the certiciatePolicies extension. Since it is absent in this certificate, what does the processing software do? Leave the

acceptable policy set as is or reset it to NULL? A setting to NULL will cause check (d) to fail and invalidate the certification path. For the validation to proceed, the absence of certiciatePolicies would have to be interpreted as having no effect on the acceptable policy set state. That is, leaving acceptable policy set as is.

```
State Variables:
    acceptable policy set: Pa, Pb, Pc
    explicit-policy-pending: 2
```

```
Signature Certificate
    Issuer: Class 3 CA-1
    Subject: Signer
    keyUsage: DS, NR                                    c = T
    certificatePolicies: Pa          qualifiers: no     c = F
    policyMappings: not used
    nameConstraints: not used
    policyConstraints: not used
```

```
State Variables:
    acceptable policy set: Pa
    explicit-policy-pending: 2
```

Status: Succeeded. All path processing checks succeeded, given the decision discussed in comment above.

Case 5: Root CA cites policies. Signing CA does not cite policies. RP cites policy Pb.

```
RP Inputs:
    Certification Path: Root - CA-1 - Signer          n = 3
    Trusted public key: Root public key
    initial-policy-set: Pb
    Current date/time
```

```
Initialize State Variables:
    acceptable policy set: any-policy
    explicit-policy-pending: 4
```

```
DoD Root CA Certificate
    Issuer: Class 3 Root CA
    Subject: Class 3 Root CA
    keyUsage: not used
    certificatePolicies: Pa, Pb, Pc  qualifiers: no  c = F
    policyMappings: not used
    basicConstraints:    cA = T    pLC = not used    c = F
    nameConstraints: not used
    policyConstraints: not used
```

```
State Variables:
    acceptable policy set: Pa, Pb, Pc
    explicit-policy-pending: 4
```

```
Signing CA Certificate 1
    Issuer: Class 3 Root CA
    Subject: Class 3 CA-1
    keyUsage: DS, KCS, cRLSign                        c = T
    certificatePolicies: not used
    policyMappings: not used
    basicConstraints:    cA = T    pLC = not used    c = T
    nameConstraints: not used
    policyConstraints:                                c = F
        requiredExplicitPolicy       SkipCerts = 0
        inhibitPolicyMapping         SkipCerts = 0
```

Comment: Path processing check (c.1) looks for the certiciatePolicies extension. Since it is absent in this certificate, what does the processing software do? Leave the

acceptable policy set as is or reset it to NULL? A setting to NULL will cause check (d) to fail and invalidate the certification path. For the validation to proceed, the absence of certiciatePolicies would have to be interpreted as having no effect on the acceptable policy set state. That is, leaving acceptable policy set as is.

State Variables:
acceptable policy set: Pa, Pb, Pc
explicit-policy-pending: 2

Signature Certificate
Issuer: Class 3 CA-1
Subject: Signer
keyUsage: DS, NR c = T
certificatePolicies: Pa qualifiers: no c = F
policyMappings: not used
nameConstraints: not used
policyConstraints: not used

Status: Failed.

Reason: Path processing check (b.1) failed. The policy identifier in the certificate, Pa, did not match the initial policy set, Pb.

X.509v4 procedure

Reference: X.509v4, The Directory: Public-Key and Attribute Certificate Frameworks, 04/00, section 10.

Case 1: Root CA does not cite policies. Signing CA cites policies. RP sets *initial-explicit-policy*.

RP Inputs:
- Certification Path: Root - CA-1 - Signer
- Trusted public key: Root public key
- *initial-policy-set*: Pa
- *initial-explicit-policy*: T
- *initial-policy-mapping-inhibit*: T
- Current date/time

Initialize State Variables:
- *authority-constrained-policy-set*: *any-policy*
- *permitted-subtrees*: *unbounded*
- *excluded-subtrees*: empty
- *explicit-policy-indicator*: T
- *path depth*: 1
- *policy-mapping-inhibit-indicator*: T
- *explicit-policy-pending*: unset
- *policy-mapping-inhibit-pending*: unset

DoD Root CA Certificate
- Issuer: Class 3 Root CA
- Subject: Class 3 Root CA
- keyUsage: not used
- certificatePolicies: not used
- policyMappings: not used
- basicConstraints: cA = T pLC = not used c = F
- nameConstraints: not used
- policyConstraints: not used

```
State Variables:
   authority-constrained-policy-set: NULL
   permitted-subtrees: unbounded
   excluded-subtrees: empty
   explicit-policy-indicator: T
   path depth: 2
   policy-mapping-inhibit-indicator: T
   explicit-policy-pending: unset
   policy-mapping-inhibit-pending: unset
```

```
Signing CA Certificate 1
    Issuer: Class 3 Root CA
    Subject: Class 3 CA-1
    certificatePolicies: Pa, Pb, Pc  qualifiers: no  c = F
    policyMappings: not used
    basicConstraints:   cA = T    pLC = not used    c = F
    nameConstraints: not used
    policyConstraints:                                c = F
        requiredExplicitPolicy       SkipCerts = 0
        inhibitPolicyMapping         SkipCerts = 0
```

```
State Variables:
   authority-constrained-policy-set: NULL
   permitted-subtrees: unbounded
   excluded-subtrees: empty
   explicit-policy-indicator: T
   path depth: 3
   policy-mapping-inhibit-indicator: T
   explicit-policy-pending: unset
   policy-mapping-inhibit-pending: unset
```

```
Signature Certificate
    Issuer: Class 3 CA-1
    Subject: Signer
    certificatePolicies: Pa          qualifiers: no  c = F
    policyMappings: not used
    basicConstraints: not used
    nameConstraints: not used
    policyConstraints: not used
```

State Variables:
authority-constrained-policy-set: NULL
permitted-subtrees: *unbounded*
excluded-subtrees: empty
explicit-policy-indicator: T
path depth: 4
policy-mapping-inhibit-indicator: T
explicit-policy-pending: unset
policy-mapping-inhibit-pending: unset

Status: Failed.

Reason: Explicit-policy-indicator is set and authority-constrained-policy-set is empty. (X.509v4, section 10.5, p 49, end-certificate check a)

Case 2: Root CA does not cite policies. Signing CA cites policies. RP does not set *initial-explicit-policy*.

RP Inputs:
- Certification Path: Root - CA-1 - Signer
- Trusted public key: Root public key
- *initial-policy-set*: Pa
- *initial-explicit-policy*: F
- *initial-policy-mapping-inhibit*: T
- Current date/time

⬇

Initialize State Variables:
- *authority-constrained-policy-set*: *any-policy*
- *permitted-subtrees*: *unbounded*
- *excluded-subtrees*: empty
- *explicit-policy-indicator*: F
- *path depth*: 1
- *policy-mapping-inhibit-indicator*: T
- *explicit-policy-pending*: unset
- *policy-mapping-inhibit-pending*: unset

⬇

DoD Root CA Certificate
- Issuer: Class 3 Root CA
- Subject: Class 3 Root CA
- keyUsage: not used
- certificatePolicies: not used
- policyMappings: not used
- basicConstraints: cA = T pLC = not used c = F
- nameConstraints: not used
- policyConstraints: not used

⬇

State Variables:
- *authority-constrained-policy-set*: NULL
- *permitted-subtrees*: *unbounded*
- *excluded-subtrees*: empty
- *explicit-policy-indicator*: F
- *path depth*: 2
- *policy-mapping-inhibit-indicator*: T
- *explicit-policy-pending*: unset
- *policy-mapping-inhibit-pending*: unset

⬇

```
Signing CA Certificate 1
    Issuer: Class 3 Root CA
    Subject: Class 3 CA-1
    certificatePolicies: Pa, Pb, Pc  qualifiers: no  c = F
    policyMappings: not used
    basicConstraints:    cA = T    pLC = not used    c = F
    nameConstraints: not used
    policyConstraints:                                c = F
        requiredExplicitPolicy       SkipCerts = 0
        inhibitPolicyMapping         SkipCerts = 0
```

```
State Variables:
   authority-constrained-policy-set: NULL
   permitted-subtrees: unbounded
   excluded-subtrees: empty
   explicit-policy-indicator: F
   path depth: 3
   policy-mapping-inhibit-indicator: T
   explicit-policy-pending: unset
   policy-mapping-inhibit-pending: unset
```

Status: Failed.

Reason: The *explicit-policy-indicator* is not set. The requiredExplicitPolicy component is present, the certification path includes a certificate issued by a nominated CA, and not all certificates in the path contain, in the certificate policies extension, an acceptable policy identifier defined by the RP (*initial-policy-set*: Pa). The nominated CA is issuer CA of the Signing CA Certificate 1, and it does not contain an acceptable policy identifier. (X.509v4, section 10.5, p 49, all certificate check a)

Case 3: Root CA cites policies. Signing CA cites policies. RP sets *initial-explicit-policy*.

RP Inputs:
- Certification Path: Root - CA-1 - Signer
- Trusted public key: Root public key
- *initial-policy-set*: Pa
- *initial-explicit-policy*: T
- *initial-policy-mapping-inhibit*: T
- Current date/time

Initialize State Variables:
- *authority-constrained-policy-set*: *any-policy*
- *permitted-subtrees*: *unbounded*
- *excluded-subtrees*: empty
- *explicit-policy-indicator*: T
- *path depth*: 1
- *policy-mapping-inhibit-indicator*: T
- *explicit-policy-pending*: unset
- *policy-mapping-inhibit-pending*: unset

DoD Root CA Certificate
- Issuer: Class 3 Root CA
- Subject: Class 3 Root CA
- keyUsage: not used
- certificatePolicies: Pa, Pb, Pc qualifiers: no c = F
- policyMappings: not used
- basicConstraints: cA = T pLC = not used c = F
- nameConstraints: not used
- policyConstraints: not used

State Variables:
- *authority-constrained-policy-set*: Pa, Pb, Pc
- *permitted-subtrees*: *unbounded*
- *excluded-subtrees*: empty
- *explicit-policy-indicator*: T
- *path depth*: 2
- *policy-mapping-inhibit-indicator*: T
- *explicit-policy-pending*: unset
- *policy-mapping-inhibit-pending*: unset

```
Signing CA Certificate 1
    Issuer: Class 3 Root CA
    Subject: Class 3 CA-1
    certificatePolicies: Pa, Pb, Pc  qualifiers: no  c = F
    policyMappings: not used
    basicConstraints:   cA = T    pLC = not used    c = F
    nameConstraints: not used
    policyConstraints:                              c = F
        requiredExplicitPolicy       SkipCerts = 0
        inhibitPolicyMapping         SkipCerts = 0
```

```
State Variables:
  authority-constrained-policy-set: Pa, Pb, Pc
  permitted-subtrees: unbounded
  excluded-subtrees: empty
  explicit-policy-indicator: T
  path depth: 3
  policy-mapping-inhibit-indicator: T
  explicit-policy-pending: unset
  policy-mapping-inhibit-pending: unset
```

```
Signature Certificate
    Issuer: Class 3 CA-1
    Subject: Signer
    certificatePolicies: Pa          qualifiers: no  c = F
    policyMappings: not used
    basicConstraints: not used
    nameConstraints: not used
    policyConstraints: not used
```

```
State Variables:
  authority-constrained-policy-set: Pa
  permitted-subtrees: unbounded
  excluded-subtrees: empty
  explicit-policy-indicator: T
  path depth: 4
  policy-mapping-inhibit-indicator: T
  explicit-policy-pending: unset
  policy-mapping-inhibit-pending: unset
```

user-constrained-policy-set: Pa

Status: Succeeded.

Case 4: Root CA cites policies. Signing CA cites policies. RP does not set *initial-explicit-policy*.

RP Inputs:
- Certification Path: Root - CA-1 - Signer
- Trusted public key: Root public key
- *initial-policy-set*: Pa
- *initial-explicit-policy*: F
- *initial-policy-mapping-inhibit*: T
- Current date/time

Initialize State Variables:
- *authority-constrained-policy-set*: *any-policy*
- *permitted-subtrees*: *unbounded*
- *excluded-subtrees*: empty
- *explicit-policy-indicator*: F
- *path depth*: 1
- *policy-mapping-inhibit-indicator*: T
- *explicit-policy-pending*: unset
- *policy-mapping-inhibit-pending*: unset

DoD Root CA Certificate
- Issuer: Class 3 Root CA
- Subject: Class 3 Root CA
- keyUsage: not used
- certificatePolicies: Pa, Pb, Pc qualifiers: no c = F
- policyMappings: not used
- basicConstraints: cA = T pLC = not used c = F
- nameConstraints: not used
- policyConstraints: not used

State Variables:
- *authority-constrained-policy-set*: Pa, Pb, Pc
- *permitted-subtrees*: *unbounded*
- *excluded-subtrees*: empty
- *explicit-policy-indicator*: F
- *path depth*: 2
- *policy-mapping-inhibit-indicator*: T
- *explicit-policy-pending*: unset
- *policy-mapping-inhibit-pending*: unset

```
Signing CA Certificate 1
    Issuer: Class 3 Root CA
    Subject: Class 3 CA-1
    certificatePolicies: Pa, Pb, Pc  qualifiers: no  c = F
    policyMappings: not used
    basicConstraints:   cA = T    pLC = not used    c = F
    nameConstraints: not used
    policyConstraints:                              c = F
        requiredExplicitPolicy       SkipCerts = 0
        inhibitPolicyMapping         SkipCerts = 0
```

```
State Variables:
  authority-constrained-policy-set: Pa, Pb, Pc
  permitted-subtrees: unbounded
  excluded-subtrees: empty
  explicit-policy-indicator: F
  path depth: 3
  policy-mapping-inhibit-indicator: T
  explicit-policy-pending: unset
  policy-mapping-inhibit-pending: unset
```

```
Signature Certificate
    Issuer: Class 3 CA-1
    Subject: Signer
    certificatePolicies: Pa          qualifiers: no  c = F
    policyMappings: not used
    basicConstraints: not used
    nameConstraints: not used
    policyConstraints: not used
```

```
State Variables:
  authority-constrained-policy-set: Pa
  permitted-subtrees: unbounded
  excluded-subtrees: empty
  explicit-policy-indicator: T
  path depth: 4
  policy-mapping-inhibit-indicator: T
  explicit-policy-pending: unset
  policy-mapping-inhibit-pending: unset
```

user-constrained-policy-set: Pa

Status: Succeeded.

Case 5: Root CA cites policies. Signing CA does not cite policies. RP sets *initial-explicit-policy*.

RP Inputs:
- Certification Path: Root - CA-1 - Signer
- Trusted public key: Root public key
- *initial-policy-set*: Pa
- *initial-explicit-policy*: T
- *initial-policy-mapping-inhibit*: T
- Current date/time

Initialize State Variables:
- *authority-constrained-policy-set*: *any-policy*
- *permitted-subtrees*: *unbounded*
- *excluded-subtrees*: empty
- *explicit-policy-indicator*: T
- *path depth*: 1
- *policy-mapping-inhibit-indicator*: T
- *explicit-policy-pending*: unset
- *policy-mapping-inhibit-pending*: unset

DoD Root CA Certificate
- Issuer: Class 3 Root CA
- Subject: Class 3 Root CA
- keyUsage: not used
- certificatePolicies: Pa, Pb, Pc qualifiers: no c = F
- policyMappings: not used
- basicConstraints: cA = T pLC = not used c = F
- nameConstraints: not used
- policyConstraints: not used

State Variables:
- *authority-constrained-policy-set*: Pa, Pb, Pc
- *permitted-subtrees*: *unbounded*
- *excluded-subtrees*: empty
- *explicit-policy-indicator*: T
- *path depth*: 2
- *policy-mapping-inhibit-indicator*: T
- *explicit-policy-pending*: unset
- *policy-mapping-inhibit-pending*: unset

```
Signing CA Certificate 1
    Issuer: Class 3 Root CA
    Subject: Class 3 CA-1
    certificatePolicies: not used
    policyMappings: not used
    basicConstraints:    cA = T    pLC = not used    c = F
    nameConstraints: not used
    policyConstraints:                                c = F
        requiredExplicitPolicy       SkipCerts = 0
        inhibitPolicyMapping         SkipCerts = 0
```

```
State Variables:
   authority-constrained-policy-set: NULL
   permitted-subtrees: unbounded
   excluded-subtrees: empty
   explicit-policy-indicator: T
   path depth: 3
   policy-mapping-inhibit-indicator: T
   explicit-policy-pending: unset
   policy-mapping-inhibit-pending: unset
```

```
Signature Certificate
    Issuer: Class 3 CA-1
    Subject: Signer
    certificatePolicies: Pa          qualifiers: no  c = F
    policyMappings: not used
    basicConstraints: not used
    nameConstraints: not used
    policyConstraints: not used
```

```
State Variables:
   authority-constrained-policy-set: NULL
   permitted-subtrees: unbounded
   excluded-subtrees: empty
   explicit-policy-indicator: T
   path depth: 4
   policy-mapping-inhibit-indicator: T
   explicit-policy-pending: unset
   policy-mapping-inhibit-pending: unset
```

Status: Failed.

Reason: Explicit-policy-indicator is set and authority-constrained-policy-set is empty. (X.509v4, section 10.5, p 49, end-certificate check a)

Case 6: Root CA cites policies. Signing CA does not cite policies. RP does not set *initial-explicit-policy*.

RP Inputs:
- Certification Path: Root - CA-1 - Signer
- Trusted public key: Root public key
- *initial-policy-set*: Pa
- *initial-explicit-policy*: F
- *initial-policy-mapping-inhibit*: T
- Current date/time

⬇

Initialize State Variables:
- *authority-constrained-policy-set*: *any-policy*
- *permitted-subtrees*: *unbounded*
- *excluded-subtrees*: empty
- *explicit-policy-indicator*: F
- *path depth*: 1
- *policy-mapping-inhibit-indicator*: T
- *explicit-policy-pending*: unset
- *policy-mapping-inhibit-pending*: unset

⬇

DoD Root CA Certificate
- Issuer: Class 3 Root CA
- Subject: Class 3 Root CA
- keyUsage: not used
- certificatePolicies: Pa, Pb, Pc qualifiers: no c = F
- policyMappings: not used
- basicConstraints: cA = T pLC = not used c = F
- nameConstraints: not used
- policyConstraints: not used

⬇

State Variables:
- *authority-constrained-policy-set*: Pa, Pb, Pc
- *permitted-subtrees*: *unbounded*
- *excluded-subtrees*: empty
- *explicit-policy-indicator*: F
- *path depth*: 2
- *policy-mapping-inhibit-indicator*: T
- *explicit-policy-pending*: unset
- *policy-mapping-inhibit-pending*: unset

⬇

```
Signing CA Certificate 1
    Issuer: Class 3 Root CA
    Subject: Class 3 CA-1
    certificatePolicies: not used
    policyMappings: not used
    basicConstraints:    cA = T    pLC = not used    c = F
    nameConstraints: not used
    policyConstraints:                                c = F
        requiredExplicitPolicy       SkipCerts = 0
        inhibitPolicyMapping         SkipCerts = 0
```

```
State Variables:
   authority-constrained-policy-set: NULL
   permitted-subtrees: unbounded
   excluded-subtrees: empty
   explicit-policy-indicator: F
   path depth: 3
   policy-mapping-inhibit-indicator: T
   explicit-policy-pending: unset
   policy-mapping-inhibit-pending: unset
```

Status: Failed.

Reason: The *explicit-policy-indicator* is not set. The requiredExplicitPolicy component is present, the certification path includes a certificate issued by a nominated CA, and not all certificates in the path contain, in the certificate policies extension, an acceptable policy identifier defined by the RP (*initial-policy-set*: Pa). The nominated CA is issuer CA of the Signing CA Certificate 1. The Signing CA Certificate 1 does not contain an acceptable policy identifier. (X.509v4, section 10.5, p 49, all certificate check a)

Case 7: Root CA cites policies. Signing CA cites policies. RP sets *initial-explicit-policy*. RP set *initial-policy-set* to Pb.

RP Inputs:
- Certification Path: Root - CA-1 - Signer
- Trusted public key: Root public key
- *initial-policy-set*: Pb
- *initial-explicit-policy*: T
- *initial-policy-mapping-inhibit*: T
- Current date/time

Initialize State Variables:
- *authority-constrained-policy-set*: *any-policy*
- *permitted-subtrees*: *unbounded*
- *excluded-subtrees*: empty
- *explicit-policy-indicator*: T
- *path depth*: 1
- *policy-mapping-inhibit-indicator*: T
- *explicit-policy-pending*: unset
- *policy-mapping-inhibit-pending*: unset

DoD Root CA Certificate
- Issuer: Class 3 Root CA
- Subject: Class 3 Root CA
- keyUsage: not used
- certificatePolicies: Pa, Pb, Pc qualifiers: no c = F
- policyMappings: not used
- basicConstraints: cA = T pLC = not used c = F
- nameConstraints: not used
- policyConstraints: not used

State Variables:
- *authority-constrained-policy-set*: Pa, Pb, Pc
- *permitted-subtrees*: *unbounded*
- *excluded-subtrees*: empty
- *explicit-policy-indicator*: T
- *path depth*: 2
- *policy-mapping-inhibit-indicator*: T
- *explicit-policy-pending*: unset
- *policy-mapping-inhibit-pending*: unset

```
Signing CA Certificate 1
    Issuer: Class 3 Root CA
    Subject: Class 3 CA-1
    certificatePolicies: Pa, Pb, Pc  qualifiers: no  c = F
    policyMappings: not used
    basicConstraints:   cA = T    pLC = not used    c = F
    nameConstraints: not used
    policyConstraints:                              c = F
        requiredExplicitPolicy       SkipCerts = 0
        inhibitPolicyMapping         SkipCerts = 0
```

```
State Variables:
  authority-constrained-policy-set: Pa, Pb, Pc
  permitted-subtrees: unbounded
  excluded-subtrees: empty
  explicit-policy-indicator: T
  path depth: 3
  policy-mapping-inhibit-indicator: T
  explicit-policy-pending: unset
  policy-mapping-inhibit-pending: unset
```

```
Signature Certificate
    Issuer: Class 3 CA-1
    Subject: Signer
    certificatePolicies: Pa          qualifiers: no  c = F
    policyMappings: not used
    basicConstraints: not used
    nameConstraints: not used
    policyConstraints: not used
```

```
State Variables:
  authority-constrained-policy-set: Pa
  permitted-subtrees: unbounded
  excluded-subtrees: empty
  explicit-policy-indicator: T
  path depth: 4
  policy-mapping-inhibit-indicator: T
  explicit-policy-pending: unset
  policy-mapping-inhibit-pending: unset
```

user-constrained-policy-set: NULL

Status: Succeeded.

Comment: There seems to be a presumption that a RP receiving a certification path validation success indication, but a NULL *user-constrained-policy-set* will understand that the policy acceptable to it (Pb) does not apply to the Signature Certificate. A comparison to *initial-policy-set* would be required.

Case 8: Root CA cites policies. Signing CA cites policies. RP does not set *initial-explicit-policy*. RP set *initial-policy-set* to Pb.

RP Inputs:
- Certification Path: Root - CA-1 - Signer
- Trusted public key: Root public key
- *initial-policy-set*: Pb
- *initial-explicit-policy*: F
- *initial-policy-mapping-inhibit*: T
- Current date/time

Initialize State Variables:
- *authority-constrained-policy-set*: *any-policy*
- *permitted-subtrees*: *unbounded*
- *excluded-subtrees*: empty
- *explicit-policy-indicator*: F
- *path depth*: 1
- *policy-mapping-inhibit-indicator*: T
- *explicit-policy-pending*: unset
- *policy-mapping-inhibit-pending*: unset

DoD Root CA Certificate
- Issuer: Class 3 Root CA
- Subject: Class 3 Root CA
- keyUsage: not used
- certificatePolicies: Pa, Pb, Pc qualifiers: no c = F
- policyMappings: not used
- basicConstraints: cA = T pLC = not used c = F
- nameConstraints: not used
- policyConstraints: not used

State Variables:
- *authority-constrained-policy-set*: Pa, Pb, Pc
- *permitted-subtrees*: *unbounded*
- *excluded-subtrees*: empty
- *explicit-policy-indicator*: F
- *path depth*: 2
- *policy-mapping-inhibit-indicator*: T
- *explicit-policy-pending*: unset
- *policy-mapping-inhibit-pending*: unset

```
Signing CA Certificate 1
    Issuer: Class 3 Root CA
    Subject: Class 3 CA-1
    certificatePolicies: Pa, Pb, Pc  qualifiers: no  c = F
    policyMappings: not used
    basicConstraints:   cA = T    pLC = not used    c = F
    nameConstraints: not used
    policyConstraints:                              c = F
        requiredExplicitPolicy       SkipCerts = 0
        inhibitPolicyMapping         SkipCerts = 0
```

```
State Variables:
  authority-constrained-policy-set: Pa, Pb, Pc
  permitted-subtrees: unbounded
  excluded-subtrees: empty
  explicit-policy-indicator: F
  path depth: 3
  policy-mapping-inhibit-indicator: T
  explicit-policy-pending: unset
  policy-mapping-inhibit-pending: unset
```

```
Signature Certificate
    Issuer: Class 3 CA-1
    Subject: Signer
    certificatePolicies: Pa          qualifiers: no  c = F
    policyMappings: not used
    basicConstraints: not used
    nameConstraints: not used
    policyConstraints: not used
```

```
State Variables:
  authority-constrained-policy-set: Pa
  permitted-subtrees: unbounded
  excluded-subtrees: empty
  explicit-policy-indicator: T
  path depth: 4
  policy-mapping-inhibit-indicator: T
  explicit-policy-pending: unset
  policy-mapping-inhibit-pending: unset
```

user-constrained-policy-set: NULL

Status: Succeeded.

Comment: There seems to be a presumption that a RP receiving a certification path validation success indication, but a NULL *user-constrained-policy-set* will understand that the policy acceptable to it (Pb) does not apply to the Signature Certificate. A comparison to *initial-policy-set* would be required.

Revised RFC 2459 procedure

Reference: draft-ietf-pkix-new-part1, Internet X.509 Public Key Infrastructure Certificate and CRL Profile, March 10, 2000, section 6.1.

Case 1: Root CA does not cite policies. Signing CA cites policies. RP sets initial-explicit-policy.

```
RP Inputs:
  Certification Path: Root - CA-1 - Signer              n = 3
  Time at which the path validity is to be determined
  user_initial_policy_set: Pa
  Trust anchor information: Root CA
        issuer name:              unique identifier, optional
               Class 3 Root CA
        public key algorithm      parameters, optional
        public key
  initial-policy-mapping-inhibit: F
  initial-explicit-policy: T
  initial-any-policy-inhibit: T
```

```
Initialize State Variables:
  valid_policy_tree:   any-policy    {}    c = F   {any-policy}
  permitted_subtrees: unbounded
  excluded_subtrees: empty
  explicit_policy: 0
  inhibit_any-policy: 0
  policy_mapping: 4
  working_public_key_algorithm: Class 3 Root CA PK algorithm
  working_public_key: Class 3 Root CA PK
  working_public_key_parameters: none
  working_issuer_name: Class 3 Root CA
  working_issuer_UID: NULL
  max_path_length: 3
```

```
DoD Root CA Certificate
    Issuer: Class 3 Root CA
    Subject: Class 3 Root CA
    keyUsage: not used
    certificatePolicies: not used
    policyMappings: not used
    basicConstraints:    cA = T    pLC = not used    c = F
    nameConstraints: not used
    policyConstraints: not used
```

```
State Variables:
   valid_policy_tree: NULL
   permitted_subtrees: unbounded
   excluded_subtrees: empty
   explicit_policy: 0
   inhibit_any-policy: 0
   policy_mapping: 4
   working_public_key_algorithm: Class 3 Root CA PK algorithm
   working_public_key: Class 3 Root CA PK
   working_public_key_parameters: none
   working_issuer_name: Class 3 Root CA
   working_issuer_UID: NULL
   max_path_length: 3
```

Status: Failed

Reason: Procedure failed at step 6.1.3(f), the explicit_policy is 0, and valid_policy_tree is equal to NULL.

Case 2: Root CA does not cite policies. Signing CA cites policies. RP does not set initial-explicit-policy.

```
RP Inputs:
  Certification Path: Root - CA-1 - Signer              n = 3
  Time at which the path validity is to be determined
  user_initial_policy_set: Pa
  Trust anchor information: Root CA
        issuer name:              unique identifier, optional
               Class 3 Root CA
        public key algorithm      parameters, optional
        public key
  initial-policy-mapping-inhibit: F
  initial-explicit-policy: F
  initial-any-policy-inhibit: T
```

```
Initialize State Variables:
  valid_policy_tree:   any-policy    {}    c = F   {any-policy}
  permitted_subtrees: unbounded
  excluded_subtrees: empty
  explicit_policy: 4
  inhibit_any-policy: 0
  policy_mapping: 4
  working_public_key_algorithm: Class 3 Root CA PK algorithm
  working_public_key: Class 3 Root CA PK
  working_public_key_parameters: none
  working_issuer_name: Class 3 Root CA
  working_issuer_UID: NULL
  max_path_length: 3
  i = 1
```

```
DoD Root CA Certificate
    Issuer: Class 3 Root CA
    Subject: Class 3 Root CA
    keyUsage: not used
    certificatePolicies: not used
    policyMappings: not used
    basicConstraints:    cA = T    pLC = not used    c = F
    nameConstraints: not used
    policyConstraints: not used
```

```
State Variables:
   valid_policy_tree: NULL
   permitted_subtrees: unbounded
   excluded_subtrees: empty
   explicit_policy: 4
   inhibit_any-policy: 0
   policy_mapping: 4
   working_public_key_algorithm: Class 3 Root CA PK algorithm
   working_public_key: Class 3 Root CA PK
   working_public_key_parameters: none
   working_issuer_name: Class 3 Root CA
   working_issuer_UID: NULL
   max_path_length: 3
   i = 2
```

```
Signing CA Certificate 1
    Issuer: Class 3 Root CA
    Subject: Class 3 CA-1
    certificatePolicies: Pa, Pb, Pc  qualifiers: no  c = F
    policyMappings: not used
    basicConstraints:   cA = T    pLC = Not used    c = F
    nameConstraints: not used
    policyConstraints:                              c = F
        requiredExplicitPolicy       SkipCerts = 0
        inhibitPolicyMapping         SkipCerts = 0
```

```
State Variables:
   valid_policy_tree: NULL
   permitted_subtrees: unbounded
   excluded_subtrees: empty
   explicit_policy: 0
   inhibit_any-policy: 0
   policy_mapping: 0
   working_public_key_algorithm: Class 3 CA-1 PK algorithm
   working_public_key: Class 3 CA-1 PK
   working_public_key_parameters: none
   working_issuer_name: Class 3 CA-1
   working_issuer_UID: NULL
   max_path_length: 2
   i = 3
```

```
Signature Certificate
    Issuer: Class 3 CA-1
    Subject: Signer
    certificatePolicies: Pa          qualifiers: no     c = F
    policyMappings: not used
    basicConstraints: not used
    nameConstraints: not used
    policyConstraints: not used
```

```
State Variables:
   valid_policy_tree: NULL
   permitted_subtrees: unbounded
   excluded_subtrees: empty
   explicit_policy: 0
   inhibit_any-policy: 0
   policy_mapping: 0
   working_public_key_algorithm: Class 3 CA-1 PK algorithm
   working_public_key: Class 3 CA-1 PK
   working_public_key_parameters: none
   working_issuer_name: Class 3 CA-1
   working_issuer_UID: NULL
   max_path_length: 2
   i = 3
```

Status: Failed.

Reason: Procedure failed at step 6.1.3(f), the explicit_policy is 0, and valid_policy_tree is equal to NULL.

Case 3: Root CA cites policies. Signing CA cites policies. RP sets initial-explicit-policy.

```
RP Inputs:
  Certification Path: Root - CA-1 - Signer              n = 3
  Time at which the path validity is to be determined
  user_initial_policy_set: Pa
  Trust anchor information: Root CA
        issuer name:              unique identifier, optional
               Class 3 Root CA
        public key algorithm      parameters, optional
        public key
  initial-policy-mapping-inhibit: F
  initial-explicit-policy: T
  initial-any-policy-inhibit: T
```

```
Initialize State Variables:
  valid_policy_tree:   any-policy    {}    c = F   {any-policy}
  permitted_subtrees: unbounded
  excluded_subtrees: empty
  explicit_policy: 0
  inhibit_any-policy: 0
  policy_mapping: 4
  working_public_key_algorithm: Class 3 Root CA PK algorithm
  working_public_key: Class 3 Root CA PK
  working_public_key_parameters: none
  working_issuer_name: Class 3 Root CA
  working_issuer_UID: NULL
  max_path_length: 3
```

```
DoD Root CA Certificate
    Issuer: Class 3 Root CA
    Subject: Class 3 Root CA
    keyUsage: not used
    certificatePolicies: Pa, Pb, Pc  qualifiers: no  c = F
    policyMappings: not used
    basicConstraints:   cA = T    pLC = not used     c = F
    nameConstraints: not used
    policyConstraints: not used
```

```
State Variables:
  valid_policy_tree:       Pa        {}    c = F      {Pa}
                           Pb        {}    c = F      {Pb}
                           Pc        {}    c = F      {Pc}
  permitted_subtrees: unbounded
  excluded_subtrees: empty
  explicit_policy: 0
  inhibit_any-policy: 0
  policy_mapping: 4
  working_public_key_algorithm: Class 3 Root CA PK algorithm
  working_public_key: Class 3 Root CA PK
  working_public_key_parameters: none
  working_issuer_name: Class 3 Root CA
  working_issuer_UID: NULL
  max_path_length: 3
  i = 2
```

```
Signing CA Certificate 1
    Issuer: Class 3 Root CA
    Subject: Class 3 CA-1
    certificatePolicies: Pa, Pb, Pc  qualifiers: no  c = F
    policyMappings: not used
    basicConstraints:   cA = T    pLC = Not used    c = F
    nameConstraints: not used
    policyConstraints:                              c = F
        requiredExplicitPolicy       SkipCerts = 0
        inhibitPolicyMapping         SkipCerts = 0
```

```
State Variables:
  valid_policy_tree:       Pa        {}    c = F      {Pa}
                           Pb        {}    c = F      {Pb}
                           Pc        {}    c = F      {Pc}
  permitted_subtrees: unbounded
  excluded_subtrees: empty
  explicit_policy: 0
  inhibit_any-policy: 0
  policy_mapping: 0
  working_public_key_algorithm: Class 3 CA-1 PK algorithm
  working_public_key: Class 3 CA-1 PK
  working_public_key_parameters: none
  working_issuer_name: Class 3 CA-1
  working_issuer_UID: NULL
  max_path_length: 2
  i = 3
```

```
Signature Certificate
    Issuer: Class 3 CA-1
    Subject: Signer
    certificatePolicies: Pa          qualifiers: no     c = F
    policyMappings: not used
    basicConstraints: not used
    nameConstraints: not used
    policyConstraints: not used
```

```
State Variables:
   valid_policy_tree:       Pa        {}    c = F       {Pa}
   permitted_subtrees: unbounded
   excluded_subtrees: empty
   explicit_policy: 0
   inhibit_any-policy: 0
   policy_mapping: 0
   working_public_key_algorithm: Signer PK algorithm
   working_public_key: Signer PK
   working_public_key_parameters: none
   working_issuer_name: Class 3 CA-1
   working_issuer_UID: NULL
   max_path_length: 2
   i = 3
```

Status: Succeeded.

Case 4: Root CA cites policies. Signing CA cites policies. RP does not set initial-explicit-policy.

```
RP Inputs:
  Certification Path: Root - CA-1 - Signer              n = 3
  Time at which the path validity is to be determined
  user_initial_policy_set: Pa
  Trust anchor information: Root CA
        issuer name:              unique identifier, optional
                Class 3 Root CA
        public key algorithm      parameters, optional
        public key
  initial-policy-mapping-inhibit: F
  initial-explicit-policy: F
  initial-any-policy-inhibit: T
```

```
Initialize State Variables:
  valid_policy_tree:   any-policy    {}    c = F   {any-policy}
  permitted_subtrees: unbounded
  excluded_subtrees: empty
  explicit_policy: 4
  inhibit_any-policy: 0
  policy_mapping: 4
  working_public_key_algorithm: Class 3 Root CA PK algorithm
  working_public_key: Class 3 Root CA PK
  working_public_key_parameters: none
  working_issuer_name: Class 3 Root CA
  working_issuer_UID: NULL
  max_path_length: 3
  i = 1
```

```
DoD Root CA Certificate
    Issuer: Class 3 Root CA
    Subject: Class 3 Root CA
    keyUsage: not used
    certificatePolicies: Pa, Pb, Pc  qualifiers: no  c = F
    policyMappings: not used
    basicConstraints:    cA = T    pLC = not used     c = F
    nameConstraints: not used
    policyConstraints: not used
```

```
State Variables:
  valid_policy_tree:       Pa        {}    c = F      {Pa}
                           Pb        {}    c = F      {Pb}
                           Pc        {}    c = F      {Pc}
  permitted_subtrees: unbounded
  excluded_subtrees: empty
  explicit_policy: 4
  inhibit_any-policy: 0
  policy_mapping: 4
  working_public_key_algorithm: Class 3 Root CA PK algorithm
  working_public_key: Class 3 Root CA PK
  working_public_key_parameters: none
  working_issuer_name: Class 3 Root CA
  working_issuer_UID: NULL
  max_path_length: 3
  i = 2
```

```
Signing CA Certificate 1
    Issuer: Class 3 Root CA
    Subject: Class 3 CA-1
    certificatePolicies: Pa, Pb, Pc  qualifiers: no  c = F
    policyMappings: not used
    basicConstraints:   cA = T    pLC = Not used    c = F
    nameConstraints: not used
    policyConstraints:                              c = F
        requiredExplicitPolicy       SkipCerts = 0
        inhibitPolicyMapping         SkipCerts = 0
```

```
State Variables:
  valid_policy_tree:       Pa        {}    c = F      {Pa}
                           Pb        {}    c = F      {Pb}
                           Pc        {}    c = F      {Pc}
  permitted_subtrees: unbounded
  excluded_subtrees: empty
  explicit_policy: 0
  inhibit_any-policy: 0
  policy_mapping: 0
  working_public_key_algorithm: Class 3 CA-1 PK algorithm
  working_public_key: Class 3 CA-1 PK
  working_public_key_parameters: none
  working_issuer_name: Class 3 CA-1
  working_issuer_UID: NULL
  max_path_length: 2
  i = 3
```

```
Signature Certificate
    Issuer: Class 3 CA-1
    Subject: Signer
    certificatePolicies: Pa          qualifiers: no     c = F
    policyMappings: not used
    basicConstraints: not used
    nameConstraints: not used
    policyConstraints: not used
```

```
State Variables:
   valid_policy_tree:       Pa        {}    c = F       {Pa}
   permitted_subtrees: unbounded
   excluded_subtrees: empty
   explicit_policy: 0
   inhibit_any-policy: 0
   policy_mapping: 0
   working_public_key_algorithm: Signer PK algorithm
   working_public_key: Signer PK
   working_public_key_parameters: none
   working_issuer_name: Class 3 CA-1
   working_issuer_UID: NULL
   max_path_length: 2
   i = 3
```

Status: Succeeded.

Case 5: Root CA cites policies. Signing CA does not cite policies. RP sets initial-explicit-policy.

```
RP Inputs:
  Certification Path: Root - CA-1 - Signer              n = 3
  Time at which the path validity is to be determined
  user_initial_policy_set: Pa
  Trust anchor information: Root CA
        issuer name:              unique identifier, optional
               Class 3 Root CA
        public key algorithm      parameters, optional
        public key
  initial-policy-mapping-inhibit: F
  initial-explicit-policy: T
  initial-any-policy-inhibit: T
```

```
Initialize State Variables:
  valid_policy_tree:   any-policy    {}    c = F   {any-policy}
  permitted_subtrees: unbounded
  excluded_subtrees: empty
  explicit_policy: 0
  inhibit_any-policy: 0
  policy_mapping: 4
  working_public_key_algorithm: Class 3 Root CA PK algorithm
  working_public_key: Class 3 Root CA PK
  working_public_key_parameters: none
  working_issuer_name: Class 3 Root CA
  working_issuer_UID: NULL
  max_path_length: 3
  i = 1
```

```
DoD Root CA Certificate
    Issuer: Class 3 Root CA
    Subject: Class 3 Root CA
    keyUsage: not used
    certificatePolicies: Pa, Pb, Pc  qualifiers: no  c = F
    policyMappings: not used
    basicConstraints:    cA = T    pLC = not used     c = F
    nameConstraints: not used
    policyConstraints: not used
```

```
State Variables:
  valid_policy_tree:       Pa        {}    c = F       {Pa}
                           Pb        {}    c = F       {Pb}
                           Pc        {}    c = F       {Pc}
  permitted_subtrees: unbounded
  excluded_subtrees: empty
  explicit_policy: 0
  inhibit_any-policy: 0
  policy_mapping: 4
  working_public_key_algorithm: Class 3 Root CA PK algorithm
  working_public_key: Class 3 Root CA PK
  working_public_key_parameters: none
  working_issuer_name: Class 3 Root CA
  working_issuer_UID: NULL
  max_path_length: 3
  i = 2
```

```
Signing CA Certificate 1
    Issuer: Class 3 Root CA
    Subject: Class 3 CA-1
    certificatePolicies: not used
    policyMappings: not used
    basicConstraints:    cA = T    pLC = Not used     c = F
    nameConstraints: not used
    policyConstraints:                                c = F
        requiredExplicitPolicy       SkipCerts = 0
        inhibitPolicyMapping         SkipCerts = 0
```

```
State Variables:
  valid_policy_tree:      NULL
  permitted_subtrees: unbounded
  excluded_subtrees: empty
  explicit_policy: 0
  inhibit_any-policy: 0
  policy_mapping: 4
  working_public_key_algorithm: Class 3 Root CA PK algorithm
  working_public_key: Class 3 Root CA PK
  working_public_key_parameters: none
  working_issuer_name: Class 3 Root CA
  working_issuer_UID: NULL
  max_path_length: 3
  i = 2
```

Status: Failed.

Reason: Procedure failed at step 6.1.3(f), the explicit_policy is 0, and valid_policy_tree is equal to NULL.

Case 6: Root CA cites policies. Signing CA does not cite policies. RP does not set initial-explicit-policy.

```
RP Inputs:
  Certification Path: Root - CA-1 - Signer              n = 3
  Time at which the path validity is to be determined
  user_initial_policy_set: Pa
  Trust anchor information: Root CA
        issuer name:              unique identifier, optional
                Class 3 Root CA
        public key algorithm      parameters, optional
        public key
  initial-policy-mapping-inhibit: F
  initial-explicit-policy: F
  initial-any-policy-inhibit: T
```

```
Initialize State Variables:
  valid_policy_tree:   any-policy    {}    c = F   {any-policy}
  permitted_subtrees: unbounded
  excluded_subtrees: empty
  explicit_policy: 4
  inhibit_any-policy: 0
  policy_mapping: 4
  working_public_key_algorithm: Class 3 Root CA PK algorithm
  working_public_key: Class 3 Root CA PK
  working_public_key_parameters: none
  working_issuer_name: Class 3 Root CA
  working_issuer_UID: NULL
  max_path_length: 3
  i = 1
```

```
DoD Root CA Certificate
    Issuer: Class 3 Root CA
    Subject: Class 3 Root CA
    keyUsage: not used
    certificatePolicies: Pa, Pb, Pc  qualifiers: no  c = F
    policyMappings: not used
    basicConstraints:    cA = T    pLC = not used     c = F
    nameConstraints: not used
    policyConstraints: not used
```

```
State Variables:
  valid_policy_tree:       Pa        {}    c = F       {Pa}
                           Pb        {}    c = F       {Pb}
                           Pc        {}    c = F       {Pc}
  permitted_subtrees: unbounded
  excluded_subtrees: empty
  explicit_policy: 4
  inhibit_any-policy: 0
  policy_mapping: 4
  working_public_key_algorithm: Class 3 Root CA PK algorithm
  working_public_key: Class 3 Root CA PK
  working_public_key_parameters: none
  working_issuer_name: Class 3 Root CA
  working_issuer_UID: NULL
  max_path_length: 3
  i = 2
```

```
Signing CA Certificate 1
    Issuer: Class 3 Root CA
    Subject: Class 3 CA-1
    certificatePolicies: not used
    policyMappings: not used
    basicConstraints:    cA = T    pLC = Not used     c = F
    nameConstraints: not used
    policyConstraints:                                c = F
        requiredExplicitPolicy       SkipCerts = 0
        inhibitPolicyMapping         SkipCerts = 0
```

```
State Variables:
  valid_policy_tree:      NULL
  permitted_subtrees: unbounded
  excluded_subtrees: empty
  explicit_policy: 0
  inhibit_any-policy: 0
  policy_mapping: 0
  working_public_key_algorithm: Class 3 CA-1 PK algorithm
  working_public_key: Class 3 CA-1 PK
  working_public_key_parameters: none
  working_issuer_name: Class 3 CA-1
  working_issuer_UID: NULL
  max_path_length: 2
  i = 3
```

```
Signature Certificate
    Issuer: Class 3 CA-1
    Subject: Signer
    certificatePolicies: Pa          qualifiers: no     c = F
    policyMappings: not used
    basicConstraints: not used
    nameConstraints: not used
    policyConstraints: not used
```

```
State Variables:
   valid_policy_tree:      NULL
   permitted_subtrees: unbounded
   excluded_subtrees: empty
   explicit_policy: 0
   inhibit_any-policy: 0
   policy_mapping: 0
   working_public_key_algorithm: Class 3 CA-1 PK algorithm
   working_public_key: Class 3 CA-1 PK
   working_public_key_parameters: none
   working_issuer_name: Class 3 CA-1
   working_issuer_UID: NULL
   max_path_length: 2
   i = 3
```

Status: Failed.

Reason: Procedure failed at step 6.1.3(f), the explicit_policy is 0, and valid_policy_tree is equal to NULL.

Case 7: Root CA cites policies. Signing CA cites policies. RP sets initial-explicit-policy. RP sets user_initial_policy_set to Pb.

```
RP Inputs:
  Certification Path: Root - CA-1 - Signer              n = 3
  Time at which the path validity is to be determined
  user_initial_policy_set: Pb
  Trust anchor information: Root CA
       issuer name:              unique identifier, optional
              Class 3 Root CA
       public key algorithm      parameters, optional
       public key
  initial-policy-mapping-inhibit: F
  initial-explicit-policy: T
  initial-any-policy-inhibit: T
```

```
Initialize State Variables:
  valid_policy_tree:   any-policy    {}    c = F   {any-policy}
  permitted_subtrees: unbounded
  excluded_subtrees: empty
  explicit_policy: 0
  inhibit_any-policy: 0
  policy_mapping: 4
  working_public_key_algorithm: Class 3 Root CA PK algorithm
  working_public_key: Class 3 Root CA PK
  working_public_key_parameters: none
  working_issuer_name: Class 3 Root CA
  working_issuer_UID: NULL
  max_path_length: 3
```

```
DoD Root CA Certificate
    Issuer: Class 3 Root CA
    Subject: Class 3 Root CA
    keyUsage: not used
    certificatePolicies: Pa, Pb, Pc  qualifiers: no  c = F
    policyMappings: not used
    basicConstraints:   cA = T    pLC = not used    c = F
    nameConstraints: not used
    policyConstraints: not used
```

```
State Variables:
  valid_policy_tree:       Pa        {}    c = F      {Pa}
                           Pb        {}    c = F      {Pb}
                           Pc        {}    c = F      {Pc}
  permitted_subtrees: unbounded
  excluded_subtrees: empty
  explicit_policy: 0
  inhibit_any-policy: 0
  policy_mapping: 4
  working_public_key_algorithm: Class 3 Root CA PK algorithm
  working_public_key: Class 3 Root CA PK
  working_public_key_parameters: none
  working_issuer_name: Class 3 Root CA
  working_issuer_UID: NULL
  max_path_length: 3
  i = 2
```

```
Signing CA Certificate 1
    Issuer: Class 3 Root CA
    Subject: Class 3 CA-1
    certificatePolicies: Pa, Pb, Pc  qualifiers: no  c = F
    policyMappings: not used
    basicConstraints:   cA = T    pLC = Not used    c = F
    nameConstraints: not used
    policyConstraints:                              c = F
        requiredExplicitPolicy       SkipCerts = 0
        inhibitPolicyMapping         SkipCerts = 0
```

```
State Variables:
  valid_policy_tree:       Pa        {}    c = F      {Pa}
                           Pb        {}    c = F      {Pb}
                           Pc        {}    c = F      {Pc}
  permitted_subtrees: unbounded
  excluded_subtrees: empty
  explicit_policy: 0
  inhibit_any-policy: 0
  policy_mapping: 0
  working_public_key_algorithm: Class 3 CA-1 PK algorithm
  working_public_key: Class 3 CA-1 PK
  working_public_key_parameters: none
  working_issuer_name: Class 3 CA-1
  working_issuer_UID: NULL
  max_path_length: 2
  i = 3
```

```
Signature Certificate
    Issuer: Class 3 CA-1
    Subject: Signer
    certificatePolicies: Pa          qualifiers: no     c = F
    policyMappings: not used
    basicConstraints: not used
    nameConstraints: not used
    policyConstraints: not used
```

```
State Variables:
   valid_policy_tree:      NULL
   permitted_subtrees: unbounded
   excluded_subtrees: empty
   explicit_policy: 0
   inhibit_any-policy: 0
   policy_mapping: 0
   working_public_key_algorithm: Signer PK algorithm
   working_public_key: Signer PK
   working_public_key_parameters: none
   working_issuer_name: Class 3 CA-1
   working_issuer_UID: NULL
   max_path_length: 2
   i = 3
```

Status: Failed.

Reason: Step 6.1.5(g)(iii) deleted the remaining valid_policy_tree node of Pa. Path processing fails because the final paragraph of 6.1.5 requires valid_policy_tree to be not NULL.

Case 8: Root CA cites policies. Signing CA cites policies. RP does not set initial-explicit-policy. RP sets user_initial_policy_set to Pb.

```
RP Inputs:
  Certification Path: Root - CA-1 - Signer              n = 3
  Time at which the path validity is to be determined
  user_initial_policy_set: Pb
  Trust anchor information: Root CA
       issuer name:              unique identifier, optional
              Class 3 Root CA
       public key algorithm      parameters, optional
       public key
  initial-policy-mapping-inhibit: F
  initial-explicit-policy: F
  initial-any-policy-inhibit: T
```

```
Initialize State Variables:
  valid_policy_tree:   any-policy    {}    c = F   {any-policy}
  permitted_subtrees: unbounded
  excluded_subtrees: empty
  explicit_policy: 4
  inhibit_any-policy: 0
  policy_mapping: 4
  working_public_key_algorithm: Class 3 Root CA PK algorithm
  working_public_key: Class 3 Root CA PK
  working_public_key_parameters: none
  working_issuer_name: Class 3 Root CA
  working_issuer_UID: NULL
  max_path_length: 3
  i = 1
```

```
DoD Root CA Certificate
    Issuer: Class 3 Root CA
    Subject: Class 3 Root CA
    keyUsage: not used
    certificatePolicies: Pa, Pb, Pc  qualifiers: no  c = F
    policyMappings: not used
    basicConstraints:   cA = T    pLC = not used    c = F
    nameConstraints: not used
    policyConstraints: not used
```

```
State Variables:
  valid_policy_tree:       Pa        {}    c = F      {Pa}
                           Pb        {}    c = F      {Pb}
                           Pc        {}    c = F      {Pc}
  permitted_subtrees: unbounded
  excluded_subtrees: empty
  explicit_policy: 4
  inhibit_any-policy: 0
  policy_mapping: 4
  working_public_key_algorithm: Class 3 Root CA PK algorithm
  working_public_key: Class 3 Root CA PK
  working_public_key_parameters: none
  working_issuer_name: Class 3 Root CA
  working_issuer_UID: NULL
  max_path_length: 3
  i = 2
```

```
Signing CA Certificate 1
    Issuer: Class 3 Root CA
    Subject: Class 3 CA-1
    certificatePolicies: Pa, Pb, Pc  qualifiers: no  c = F
    policyMappings: not used
    basicConstraints:   cA = T    pLC = Not used    c = F
    nameConstraints: not used
    policyConstraints:                              c = F
        requiredExplicitPolicy       SkipCerts = 0
        inhibitPolicyMapping         SkipCerts = 0
```

```
State Variables:
  valid_policy_tree:       Pa        {}    c = F      {Pa}
                           Pb        {}    c = F      {Pb}
                           Pc        {}    c = F      {Pc}
  permitted_subtrees: unbounded
  excluded_subtrees: empty
  explicit_policy: 0
  inhibit_any-policy: 0
  policy_mapping: 0
  working_public_key_algorithm: Class 3 CA-1 PK algorithm
  working_public_key: Class 3 CA-1 PK
  working_public_key_parameters: none
  working_issuer_name: Class 3 CA-1
  working_issuer_UID: NULL
  max_path_length: 2
  i = 3
```

```
Signature Certificate
    Issuer: Class 3 CA-1
    Subject: Signer
    certificatePolicies: Pa          qualifiers: no     c = F
    policyMappings: not used
    basicConstraints: not used
    nameConstraints: not used
    policyConstraints: not used
```

```
State Variables:
   valid_policy_tree:      NULL
   permitted_subtrees: unbounded
   excluded_subtrees: empty
   explicit_policy: 0
   inhibit_any-policy: 0
   policy_mapping: 0
   working_public_key_algorithm: Signer PK algorithm
   working_public_key: Signer PK
   working_public_key_parameters: none
   working_issuer_name: Class 3 CA-1
   working_issuer_UID: NULL
   max_path_length: 2
   i = 3
```

Status: Failed.

Reason: Step 6.1.5(g)(iii) deleted the remaining valid_policy_tree node of Pa. Path processing fails because the final paragraph of 6.1.5 requires valid_policy_tree to be not NULL.